

FORM PTO-1449 (MODIFIED)

LIST OF PUBLICATIONS FOR
APPLICANT'S INFORMATION
DISCLOSURE STATEMENT

Applicant(s): Philip D. MacKenzie
 Case: 15
 Serial No.: 10/600,687
 Filing Date: June 20, 2003
 Group: To Be Assigned

U.S. PATENT DOCUMENTS

EXAMINER <u>INITIAL</u>	DOCUMENT NO.	DATE	NAME	CLASS/SUBCLASS	FILING DATE IF APPROPRIATE
----------------------------	--------------	------	------	----------------	-------------------------------

FOREIGN PATENT DOCUMENTS

EXAMINER <u>INITIAL</u>	DOCUMENT NO.	DATE	COUNTRY	CLASS/SUBCLASS	TRANSLATION YES NO
----------------------------	--------------	------	---------	----------------	----------------------------

OTHER DOCUMENTS

EXAMINER <u>INITIAL</u>	REF NO.	AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.
----------------------------	---------	--

- LLS 1. V. Shoup et al., "Securing Threshold Cryptosystems against Chosen Ciphertext Attack," EUROCRYPT '98, pp. 1-22, 1998.
- LLS 2. R. Canetti et al., "An Efficient *Threshold* Public Key Cryptosystem Secure against Adaptive Chosen Ciphertext Attack," EUROCRYPT '99 (LNCS 1592), pp. 90-105, 1999.
- LLS 3. M. Abe, "Robust Distributed Multiplication without Interaction," CRYPTO '99 (LNCS 1666), pp. 130-147, 1999.
- LLS 4. S. Jarecki et al., "Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures," EUROCRYPT 2000 (LNCS 1807), pp. 221-242, 2000.
- LLS 5. P-A. Fouque et al., "Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks," ASIACRYPT '01 (LNCS 2248), pp. 351-368, 2001.
- LLS 6. M. Bellare et al., "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," 1st ACM Conference on Computer and Communications Security, pp. 62-73, November 1993.
- LLS 7. R. Canetti et al., "The Random Oracle Methodology, Revisited," 30th ACM Symposium on Theory of Computing, pp. 209-218, 1998.
- LLS 8. R. Cramer et al., "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack," CRYPTO '98 (LNCS 1462), pp. 13-25, 1998.

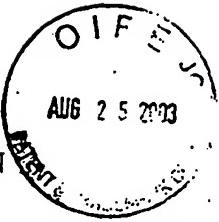
Examiner

Date Considered

/Linh Son/01/05/2007

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

FORM PTO-1449 (MODIFIED)

LIST OF PUBLICATIONS FOR
APPLICANT'S INFORMATION
DISCLOSURE STATEMENT

Applicant(s): Philip D. MacKenzie
 Case: 15
 Serial No.: 10/600,687
 Filing Date: June 20, 2003
 Group: To Be Assigned

OTHER DOCUMENTS (cont'd.)

EXAMINER	INITIAL	REF NO.	AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.
LLS			9. R. Cramer et al., "Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption," EUROCRYPT 2001 (LNCS 2332), pp. 45-64, 2002.
LLS			10. S. Micali, "Fair Public-key Cryptosystems," CRYPTO '92 (LNCS 740), pp. 113-138, 1992.
LLS			11. N. Asokan et al., "Optimistic Protocols for Fair Exchange," 3 rd ACM Conference on Computer and Communications Security, pp. 1-23, 1996.
LLS			12. P. MacKenzie et al., "Networked Cryptographic Devices Resilient to Capture," DIMACS Technical Report 2001-19, pp. 1-38, May 2001.
LLS			13. P. MacKenzie et al., "Two-Party Generation of DSA Signatures," CRYPTO 2001 (LNCS 2139), pp. 137-154, 2001.
LLS			14. R. Cramer et al., "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols," CRYPTO '94 (LNCS 839), pp. 174-187, 1994.
LLS			15. U. Feige et al., "Witness Indistinguishable and Witness Hiding Protocols," 22 nd ACM Symposium on Theory of Computing, pp. 416-426, 1990.
LLS			16. T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Volume 31, pp. 469-472, 1985.
LLS			17. J. Camenisch et al., "Proof Systems for General Statements about Discrete Logarithms," Technical Report TR 260, Department of Computer Science, ETH Zurich, pp. 1-13, March 1997.
LLS			18. I. Damgård, "Efficient Concurrent Zero-Knowledge in the Auxiliary String Model," EUROCRYPT 2000 (LNCS 1807), pp. 418-430, 2000.
LLS			19. A. Fiat et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," CRYPTO '86 (LNCS 263), pp. 186-194, 1987.

Examiner

Date Considered

/Linh Son/

01/05/2007

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.